2-10-2017

AnonPri: A Secure Anonymous Private Authentication Protocol for RFID Systems

Farzana Rahman
James Madison University

Md. Endadul Hoque
Purdue University

Sheikh Iqbal Ahamed
Marquette University, sheikh.ahamed@marquette.edu

Accepted version. *Information Sciences*, Vol. 379 (February 10, 2017): 195-210. DOI.

Information Sciences, Vol. 379, (February 10, 2017): 195-210. DOI.

AnonPri: A secure anonymous private authentication protocol for RFID systems

Farzana Rahman
Department of Computer Science, James Madison University, Harrisonburg, VA
Md Endadul Hoque
Department of Computer Science, Purdue University, West Lafayette, IN
Sheikh Iqbal Ahamed
Department of Mathematics, Statistics and Computer Science, Marquette University, Milwaukee, WI

Abstract

Privacy preservation in RFID systems is a very important issue in modern day world. Privacy activists have been worried about the invasion of user privacy while using various RFID systems and services. Hence, significant efforts have been made to design RFID systems that preserve users' privacy. Majority of the privacy preserving protocols for RFID systems require the reader to search all tags in the system in order to identify a single RFID tag which not efficient for large scale systems. In order to achieve high-speed authentication in large-scale RFID systems, researchers propose tree-based approaches, in which any pair of tags share a number of key components. Another technique is to perform group-based authentication that improves the tradeoff between scalability and privacy by dividing the tags into a number of groups. This novel authentication scheme ensures privacy of the tags. However, the level of privacy provided by the scheme decreases as more and more tags are compromised. To address this issue, in this paper, we propose a group based anonymous private authentication protocol (AnonPri) that provides higher level of privacy than the above mentioned group based scheme and achieves better efficiency (in terms of providing privacy) than the approaches that prompt the reader to perform an exhaustive search. Our protocol guarantees that the adversary cannot link the tag responses even if she can learn the identifier of the tags. Our evaluation results demonstrates that the level of privacy provided by AnonPri is higher than that of the group based authentication technique.

Keywords

Anonymity, Authentication, Privacy, RFID, Security, Unlinkibility

1. Introduction

Radio Frequency Identification (RFID) systems are becoming the most possible successor of barcode and are starting to be used in many different applications. RFID systems have been studied actively and frequently in pervasive computing environments for during last decade. It is a latest technology that eases automated recognition and has emerged as a feasible solution for identifying large quantities of item. One of the major remuneration of such a system is that human intervention is eliminated and a large number of items can be identified within little time. Evaluating the benefits of RFID begins not only with a full understanding of how the technology works, but also an appreciation of how the implementation of the technology saves time, reduces handling and labor costs, cuts cycle times, eliminates errors, and improves overall quality.

However, the expansion of RFID technology is limited because of security and privacy concerns. Conventional security primitives cannot be integrated in RFID tags as they have inadequate computation capabilities with extremely limited resources. Hence, before the enormous deployment of RFID tags in omnipresent environment, security and privacy issues must be addressed. The inherent capability of precise and reliable identification attracts RFID systems in the area of tracking applications. This potentiality, however, can put individual privacy at a risk. A threat to consumer privacy is one of the major obstacles in the widespread deployment of RFID systems. A field trial of RFID embedded loyalty cards in Europe was cancelled due to consumer protest over privacy concerns.[5] Another legal law violation have been reported against RFID application tracking kids on school buses, even though the RFID chips were installed on the buses for better route navigation and communication purposes.[27] The use of RFID chips in retail industry have been negatively reported and protested recently all over North America.[28] Additionally, plenty of healthcare applications using RFID chips are always facing controversy form consumer and government due to potential privacy leakage of its users.[29,12] Many RFID based tracking applications used in E-Passports, consumer shopping, smart keys, such everyday applications have gone through strong opposition from users, and policy makers since there are potential chances of privacy violation.[12] Strong authentication can be a solution to such privacy problems. One party (*prover*) has to prove its own identity to another party (*verifier*) in such way that an adversary can neither identify nor track the party (prover). Here, the tag is the prover and the reader is the verifier.

To address the privacy problem of RFID system, the tag has to obfuscate its identity from eavesdroppers in such a way that only the valid reader can understand and identify the tag. Encrypting the tag's message can protect its privacy. However, this technique cannot provide any hint to the reader about the key that the tag is using to encrypt its message. Therefore, the reader has to search among a set of candidate keys until it finds the right key that correctly decrypts the tag's message. As a result, the reader becomes inefficient in terms of identifying a single tag since it has to search a number of keys. This problem is intensified when the number of tags in the system increases.

Several private authentication schemes proposed in[16,26,36] provide strong privacy at the cost of the search complexity on the reader's side. In these protocols, the workload of the reader increases linearly with the number of tags in the system. In other words, the search complexity is $O(N)$, where N is the total number of tags in the system. These approaches become infeasible in some applications, such as tracking each product at every stage of supply chain management or automated display of flight information on smart tickets, where there is a huge of number of tags in the system.

Molnar and Wagner5 first proposed a tree based hash protocol for RFID systems to reduce the search complexity of the reader from $O(N)$ to $O(\log_{\alpha}N)$, where α is the branching factor at each level of the tree. The tag has to always perform $\log_{\alpha}N$ encryptions for every authentication. However, for authenticating a single tag, the worst case complexity of the reader is reduced to $\alpha\log_{\alpha}N$. But this approach achieves better scalability at the cost of some privacy loss of the tags.[25] Despite the privacy loss, the RFID community has held this protocol in great consideration because this is the first private authentication protocol that reduces the complexity of the reader. Therefore, improving the tradeoff between scalability and privacy of RFID systems has a great significance in reality. In,[4] the authors proposed a modified version of the tree based protocol where the branching factors are different at different levels of the tree. This approach improves the overall provided privacy. The authors also propose an algorithm to determine the optimal key tree for a given number of tags. Later, Avoine et al.[3] proposed a group based private authentication scheme that improves the tradeoff between scalability and privacy by dividing the tags into a number of groups. A benefit of this approach is that the tag has to perform only two encryptions for every authentication. In addition, this approach provides significant improvement in privacy protection. A serious limitation of this protocol is that whenever any tag is compromised (the group key and the tag's key become known to the adversary), all other tags of the same group lose their complete privacy. The level of privacy provided by the scheme decreases as more and more tags are compromised.

1.1. Summary of contributions

Our major contributions in this paper are as follows:

- In this paper, we provide a new insight on the privacy issue of RFID systems. We use an experiment-based definition to formalize RFID privacy from the perspective of unlinkability among different RFID tags. Our idea is to preserve privacy by introducing the notion that adversary cannot break unlinkability or invade privacy with probability better than random guessing.
- We present a group based anonymous private authentication protocol (AnonPri) as a solution to the tradeoff between the scalability and privacy problem of RFID systems. AnonPri uses symmetric key encryption and provides higher level of privacy than the above mentioned group based scheme and achieves better efficiency (in terms of disclosing less information) than the approaches that prompt the reader to do exhaustive search. Note, our proposal AnonPri is also a group based authentication protocol as the one proposed by Avoine[3] except it uses different techniques to provide better privacy and ensure more security in an RFID system. Hence, we compared the performance of AnonPri with the group based authentication protocol presented in.[3]
- Based on the notion of RFID privacy, we prove that AnonPri protects privacy of RFID tags and thereby the privacy of tag holders. We also prove that AnonPri provides unlinkability and thereby preserves privacy. The adversary cannot link the tag responses, even if she can decrypt the first portion of the response and learn the identifier that the tags are using to produce the response.

Note, we approach RFID privacy both from modeling and from protocol point of view. Our privacy model avoids the drawbacks of several proposed RFID privacy models that either suffer from insufficient generality or put forward unrealistic assumptions regarding the adversary's ability to corrupt tags. Furthermore, our model can guarantee unlikibility among tags. By privacy assurance, in our system, we refer to the notion that adversary is not able to identify which output was send by which tag. By unlinkibility, we refer to the notion that adversary is not able to distinguish between two tag outputs.

The rest of the paper is organized as follows. Section 2 reviews important privacy protection approaches proposed so far in RFID systems. In Section 3 we discuss the details of our system model. We present the AnonPri protocol in Section 4. The attack model is presented in Section 5. Subsequently, we present the privacy model in Section 6. In Section 7, we formally prove that our protocol preserves data privacy and provides unlinkability. In Section 8, we measure the level of privacy achieved by AnonPri as a function of the total number of compromised tags. In Section 9, we discuss the limitation of AnonPri. We present relevant related work in Section 10. Finally, we conclude the paper in Section 11.

2. Privacy in RFID systems

2.1. Privacy vs. scalability

Ensuring strong privacy imposes a higher complexity on the reader. On the other hand, improving efficiency may hamper some privacy. In this paper, we focus on this major problem between privacy and scalability problem of RFID systems. Public key cryptography would be a better candidate to solve the problem between privacy and scalability. In this approach, the tag would encrypt its message using the public key of the reader so that only the real reader would be able to decrypt the message and identify the tag. However, public key encryption is too expensive for low cost tags. Since we consider low cost tags that are capable of doing symmetric key encryption, our proposal is based on symmetric key encryption. In this section, first, we outline how the tree based hash protocol provides scalability but sacrifice some privacy. Next, we describe how the group based protocol provides improved scalability as well as a higher level of privacy. Finally, we point out the privacy problem of this group based protocol.

Tree based hash protocol: The tree based hash protocol proposed by Molnar and Wagner[20] reduces the reader's complexity from $O(N)$ to $O(\log_\alpha N)$. Tags are organized in a secret key tree where each tag is assigned to a leaf of the tree. Secret keys are associated with each branch of the tree. Each tag (each leaf) receives all the secret keys along the path from the root to itself. If the tree has L levels, each tag stores L keys. The authors[20] proposed the key tree as a balanced tree. So if the branching factor is α, the $\log_\alpha N$ will be equal to L. Each tag has only one key that is not shared with any other tag of the system. Fig. 1 shows a balanced key tree with $N = 8$ and $\alpha = 2$.

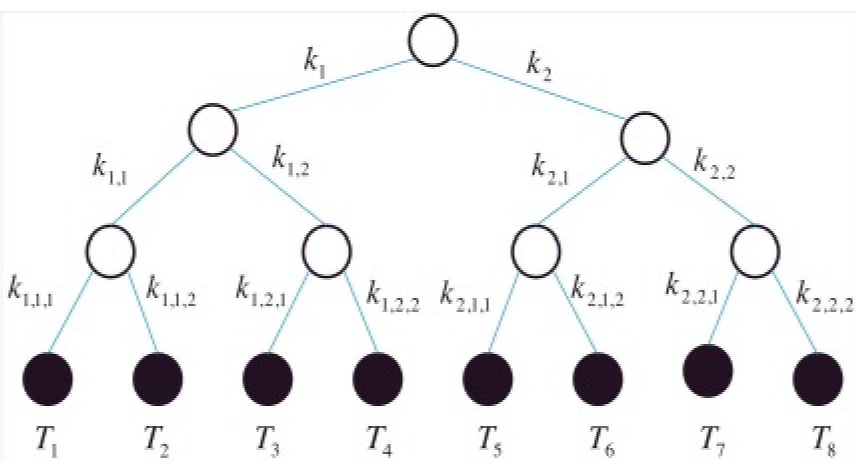


Fig. 1. A secret key tree for the tree based hash protocol with $N = 8$ and $\alpha = 2$.

According to this protocol, the reader queries a tag with a nonce n_r. Upon the reception of the nonce from the reader, the tag generates another nonce n_t and replies to the reader with

$$n_t, h(k_{l_1} \parallel n_r \parallel n_t), h(k_{l_1,l_2} \parallel n_r \parallel n_t), \ldots, h(k_{l_1,l_2,\ldots,l_L} \parallel n_r \parallel n_t),$$

Where, each $l_i \in \{1, \ldots, \alpha\}$ $1 \le i \le L$, $h(.)$ is a hash function and ∥ represents concatenation. The nonce produced by the tag provides unlinkability between two consecutive responses from the same tag. On the other side, the nonce from the reader prevents replay attacks. After receiving the response, the reader first finds a match with the first hash value of the response by hashing with all the keys of level 1. Whenever the reader obtains a match, the reader starts to search for the second hash value of the response by hashing with all the keys at the next level of the sub-tree rooted at the node where the reader has found the match. The reader repeats this step until it reaches a leaf. Thus, the reader's complexity is reduced to $O(\log_\alpha N)$. In worst case, the reader has to search with all keys at each level of the tree and therefore, the complexity becomes $\alpha \log_\alpha N$.

The major drawback of this approach is the loss of privacy if the adversary compromises any tag. Since the tags share keys with some of the tags in the system, whenever a single tag becomes compromised all the tags that share at least one key with the compromised tag have to sacrifice their privacy. Suppose the tag T_3 in Fig. 1 becomes compromised. All the tags of the system are partitioned into three disjoint sets. The adversary can now uniquely distinguish the tag T_4 and identify the tags T_1 and T_2 as a unique partition. All the remaining tags (T_5, T_6, T_7, T_8) form a single partition because the tag T_3 shares no key with them. Therefore each tag of this partition (T_5, T_6, T_7, T_8) is anonymous among these four tags. The privacy provided by this scheme diminishes as more and more tags are compromised by the adversary.

Group based protocol: Avoine et al.[3] proposed a group based authentication protocol to address the privacy problem of the tree based hash protocol. According to this protocol, tags are divided into γ disjoint groups of equal size. Each group is associated with a unique key that we refer to as a group key. Every tag shares this group key with other members of the given group. Each tag is assigned a unique key that is known only to the tag and the reader. Fig. 2 shows the group organization of the tags where $N = 8$ and $\gamma = 4$. The k_i's are the group keys, where $1 \le i \le \gamma$. The identifier of the *jth* tag is represented by ID_j (not shown in Fig. 2) and the unique secret key of the same tag is denoted as k_{T_j}, where $1 \le j \le 8$.

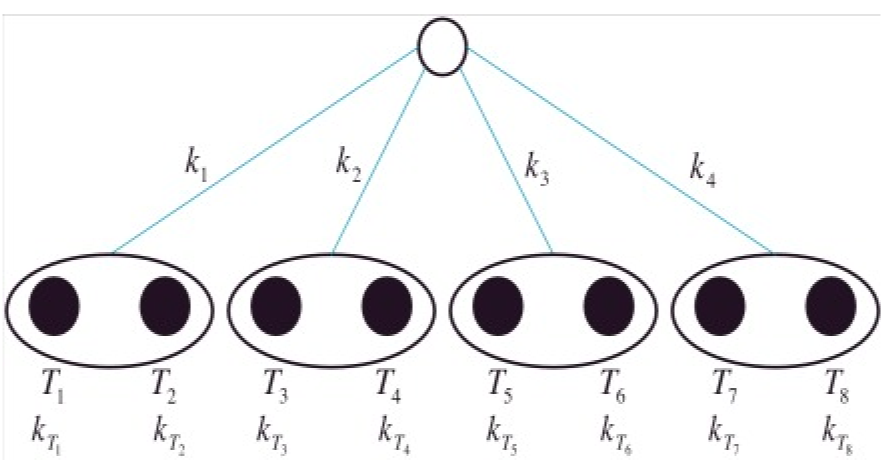


Fig. 2. Group organization of the tags for the group based authentication protocol, with $N = 8$ and $\gamma = 4$.

According to this protocol, the reader queries the tag with a nonce n_r. The tag, then, replies the following encrypted message (we assume that each tag has the knowledge of the encryption algorithm) with the nonce n_t produced by the tag $E_{k_i}(n_r \parallel n_t \parallel ID_j) \parallel E_{k_{T_j}}(n_r \parallel n_t)$.

Now the reader tries all the group keys to decrypt the first portion of the message. If the reader finds the right key that correctly decrypts the message, then the reader can learn ID_j and decrypt the following portion of the response with the secret key of the tag T_j. Thus, the reader verifies the tag's legitimacy. This protocol reduces the complexity of both the reader and the tag. The tag always has to perform two encryptions. In the worst case, the reader has to perform $\gamma + 1$ encryptions. In addition, each tag needs to store only two keys for the authentication.

The group organization of this protocol improves the level of privacy. If the adversary compromises any tag then this only effects the other members of its group. After compromising the tag, the adversary learns the group key and the tag's secret key. Now the adversary can uniquely identify every single tag from the same group since the adversary can discover each tag's identifier by decrypting the first portion of the response from each tag with the learned group key. All the remaining tags that belong to different groups form a single partition so the adversary cannot distinguish the tags that belong to this partition. For instance, if the tag T_3 is compromised, the adversary can uniquely identify only the tag T_4 (see Fig. 2). The adversary cannot uniquely distinguish the other tags T_1, T_2, T_5, T_6, T_7, T_8. Each of these tags remains anonymous among these six tags. This is a significant improvement in privacy protection of RFID systems in comparison with other protocols including tree based protocol.

Like other protocols, this protocol also has some limitations. There is a tradeoff between the number of groups and the group size. To address this problem, we propose an efficient anonymous private authentication (AnonPri) scheme that improves the privacy protection by keeping the reader's complexity moderate. In our approach, each tag is assigned to a couple of unique identifiers. A single tag shares some of its identifiers with some members of its group. Hence, this protocol prevents tracking by increasing the uncertainty of the adversary. Please note, here the identifiers should not be confused with tag keys. Identifiers are like names or IDs for tags. Disclosure of the identifiers means loss of privacy. On the other hand, tag key or key is a unique key that follows cryptographic properties and is secretly shared between the tag and reader. Tag key is used for symmetric encryption between the tag and reader in our system.

2.2. Privacy characterization

In literature, several different notions of privacy have been proposed so far. Some authors mention *information privacy* as the privacy of RFID systems. This privacy notion is the act of preventing a tag from disclosing its product information.[36,26] However, protecting information privacy keeps tags traceable. Therefore, it is a weak notion of RFID privacy. Some define *unlinkability* as the strong notion of RFID privacy.[25,6] Unlinkability means the inability to distinguish between the responses from the same tag and the responses from different tags of the system. Providing unlinkability ensures strong privacy when the adversary cannot distinguish between two tags with a probability better than random guessing.[16] In our protocol, we protect privacy of the tags by providing unlinkability between two tags of the system.

The level of privacy obtained by any protocol can be measured using the *anonymity set. Anonymity* has been proposed in the context of mix-nets in.[8] Mix-nets are used to make the sender (and the recipient) of a message anonymous. The anonymity set is defined as the set of all potential senders (recipients) of the message. Anonymity is defined as being not identifiable among a group of entities, i.e., the members of the anonymity set. A higher degree of anonymity is achieved with an anonymity set of larger size. Perfect anonymity is achieved if anonymity set contains all the members capable of sending (receiving) messages in system.

3. System model

In this section, we describe the various actors/components of our system. There are three major actors - Issuer, Tag and Reader- in our system. We also describe some key concepts that will be used throughout the rest of the paper like Group, Group Key, Tag secret key, Identifiers and System parameters. All these form the system model for AnonPri protocol.

Our protocol is based on the group-based scheme. In our system, tags are divided into groups of equal size. Suppose, N is the total number of tags in the system and τ is the number of groups. So, the group size is $n = \frac{N}{\tau}$. In this section, we define the components and parameters of our system.

Issuer. The issuer initializes each tag during the deployment by writing the tag's information into its memory. The issuer also authorizes the reader access to the tags. Even each group receives its unique group key and a pool of identifiers from the issuer.

Group. Each group has a n number of tags. The issuer assigns a unique group key k_{G_i} to the ith group G_i of the system. This key is shared between the members (tags) of this group. Each group also receives the following pool of identifiers from the issuer $\xi_i = \{ID_{i,1}, ID_{i,2}, \ldots, ID_{i,M}\}$, where, $1 \le i \le \tau$ and M is a system parameter. The pools of any two groups do not share any identifier, i.e., $\xi_i \cap \xi_j = \emptyset, \forall i \neq j$. Each tag of the group G_i is assigned a couple of identifiers from ξ_i by the issuer.

Tag. All the tags of the system are divided into τ groups. Each tag receives the shared group key of the group that the tag belongs to, a unique secret key that is known only to the reader and the tag itself, and a set of identifiers from the pool of identifiers of the group. Suppose, the tag T_j belongs to the group G_i. This tag possesses the group key k_{G_i}, the unique secret key k_{T_j}, and a set of identifiers Ω_{ij}. Each key is of ϑ bits, where ϑ is the security parameter of symmetric key encryption. We define the Ω_{ij} as follows where,

- each ID_{i,j_x} is chosen randomly following uniform distribution from the pool ξ_i and $j_x \in \{1,2,\ldots,M\}$, where $1 \leq x \leq m$
- $ID_{i,j_x} \neq ID_{i,j_y}$, for all $x \neq y$
- m is also a system parameter and $M > m$.
- Here, M is a system parameter that refers to the number of identifiers assigned to a particular group. And m refers to the number of identifiers assigned to each tag. The more identifiers are assigned, that is the more the value of M, the harder it is for the adversary to break privacy. However, we cannot make M such a very large number so that the system becomes slow. There has to be a tradeoff between the two and system designer needs to make a decision of choosing M based on the requirement of system's performance and privacy need.

To ensure that attacker cannot find out which identifier belongs to which tag, in our system we let identifiers to be shared between multiple tags within a group. By allowing a single identifier to be shared by multiple tags within a group, we make sure that attacker finds those tags unlinkable from each other, hence guaranteeing more privacy than traditional protocols. In our system, the identifiers are assigned to the tags in such a way that at least one identifier of a tag is shared with at least two other members of the same group.

So, we can say for the tag T_j, $\exists p,q[ID_{i,j_x} \in (\Omega_{ip} \cap \Omega_{iq})]$,

Where, p,q are any two members of G_i and $p \neq q$.

Reader. The reader is connected to the backend server. In this paper, we assume the communication channel between the reader and the backend server is secured. From now on, we denote the backend server as the reader. In our system, the tag is the prover and the reader is the verifier. The reader receives all the secret information by the issuer during the deployment. The issuer issues the reader a set of secret information for each group in the system $\psi = \{k_{G_i}, \sigma_i | 1 \leq i \leq \tau\}$, where k_{G_i} is the secret group key and σ_i is the mapping of the identifiers of the pool ξ_i with the secret keys of tags. Formally, $\sigma_i = \{ID_{i,x}, \pi_x | 1 \leq x \leq M \text{ and } ID_{i,x} \in \xi_i\}$,

Where, π_x is the set of secret keys of tags associated with the $ID_{i,x}$. π_x can be defined as an empty set if no tag is associated with the $ID_{i,x}$ or it can be a set of size at least one. Formally,

$$\pi_x = \begin{cases} \{k_{\omega_1}, k_{\omega_2}, \ldots\}, & where \omega_* \in \{T_1, T_2, \ldots, T_N\} \\ \emptyset, & otherwise \end{cases}.$$

System parameters. Since each tag receives m identifiers randomly chosen from the pool of M identifiers, according to the ID distribution strategy, we can say that each tag has at least one identifier common with at least two group members. The probability that each tag shares at least one identifier with at least two group members is

$$P_{share} = 1 - \left(\frac{\binom{M-m}{m}}{\binom{M}{m}} \times \frac{\binom{M-2m}{m}}{\binom{M}{m}}\right) = 1 - \frac{((M-m)!)^3}{(M!)^2(M-3m)!}$$

Where, $M \geq nm$. For example, we consider an RFID system of 1000 tags divided in 10 groups. 100 tags are in each group. For simplicity, we assume M = 1000 and m = 10. Then the probability that each tag shares at least one identifier with at least two group members is $P_{share} = 96.87\%$.

4. Our protocol: AnonPri

In this section, we describe our protocol. In our protocol, in order to authenticate a tag, the reader sends a single challenge to the tag. The answer of the tag has two parts. In the first part, the tag answers to the reader by encrypting with the group key the reader's challenge concatenated with a nonce picked by the tag, and the tag's identifier (chosen from the pool of IDs). In the second part, the tag encrypts the challenge concatenated with the nonce using its own secret key. Encrypting the identifier is needed since the key used for encryption does not identify uniquely the tag. Upon reception of the answer, the reader identifies the tag by trying all the group keys until the decryption succeeds. Once the reader finds out the tag ID, then it checks the second part. The reader tries all secret keys associated with the identifier to decrypt the second part of the message. Without the second part, every tag could impersonate every other tag in the same group. Fig. 3 illustrates the two party message communications in AnonPri.

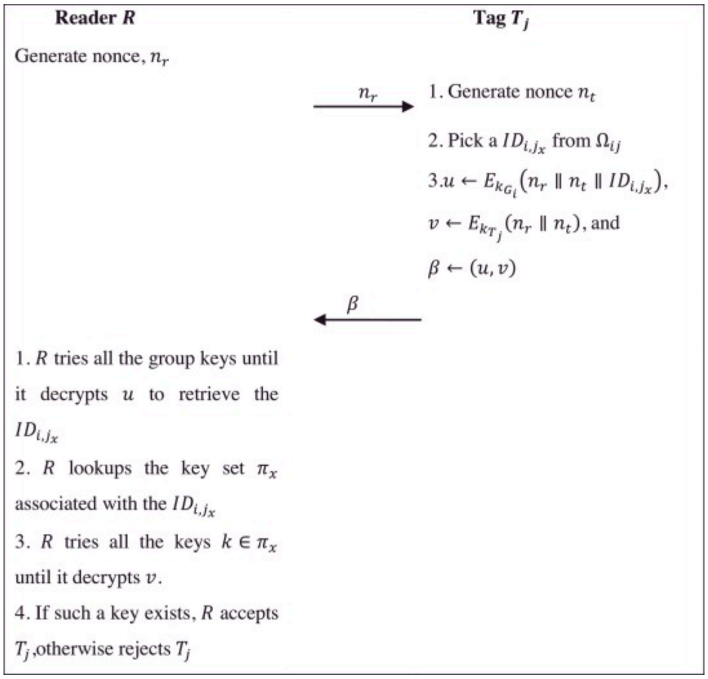


Fig. 3. The anonymous private authentication protocol (AnonPri).

The reader starts to query the tag with a nonce n_r. Upon the reception of the query, the tag generates another nonce n_t. Suppose the reader interrogates the tag T_j. In the second step, the tag picks an identifier, say ID_{i,j_x}, from Ω_{ij}. Then the tag computes β as shown in Fig. 3. Here, $E_k(.)$ denotes symmetric key encryption with key k. The tag replies with the β. Now the reader searches all the group keys until it finds the correct one that properly decrypts the first part (u) of the response. If the reader retrieves the identifier ID_{i,j_x} that the tag used in its response, then the reader tries to decrypt the second part (v) of β with the potential set of secret keys (π_x) associated with ID_{i,j_x}. After finding the right secret key, the reader can uniquely identify the tag T_j. Sharing some identifiers of a tag with other members of the group provide unlinkability even if any tag is compromised by the adversary. We discuss this in section VII.

5. Attack model

In this section and the following section, we discuss how AnonPri guarantees the privacy and security of an RFID system. We first define the attack model in our system. Then we define the two key concept, privacy and unlinkibility, from the perspective of AnonPri and finally we demonstrate the ability of AnonPri in defending against physical attacks, which in turn ensures more privacy and guarantees unlinkibility.

One of the major goals of an adversary in any RFID system is to infringe the tags' privacy by means of tracking. Our attack model (shown in Fig. 4) allows the adversary to eavesdrop on the communication between tags and the reader, and also to communicate directly with the tag and the reader, but not to modify messages that are sent between them. In other words, we consider an active adversary, but explicitly disregard man-in-the-middle attacks. In this paper, an adversary is denoted as $\hat{A}$. We assume $\hat{A}$ as an active adversary who has full control over all the communications between the tag and the reader. She can not only eavesdrop, but also intercept, modify and even initiate authentication session. The adversary can, for example, impersonate a tag and communicate with the valid reader. Even the adversary can query a valid tag and learn the tag's response. Our assumptions also include that the adversary can control a number of readers and tags. Each reader and tag controlled by the adversary are denoted as $\hat{R}$ and $\hat{T}$, respectively. $\hat{R}$ is unauthorized to have access to any real tags since $\hat{R}$ has no secret information like the real reader R. Similarly, $\hat{T}$ is not valid as it does not have the secret and identifying information of a valid tag. However, the adversarial reader $\hat{R}$ can communicate with a valid tag. Even the fake tag $\hat{T}$ can communicate with a legitimate reader. In both cases, the ultimate goal of the adversary is to track any tag of the system. Fig. 4 illustrates the attack model in our system:

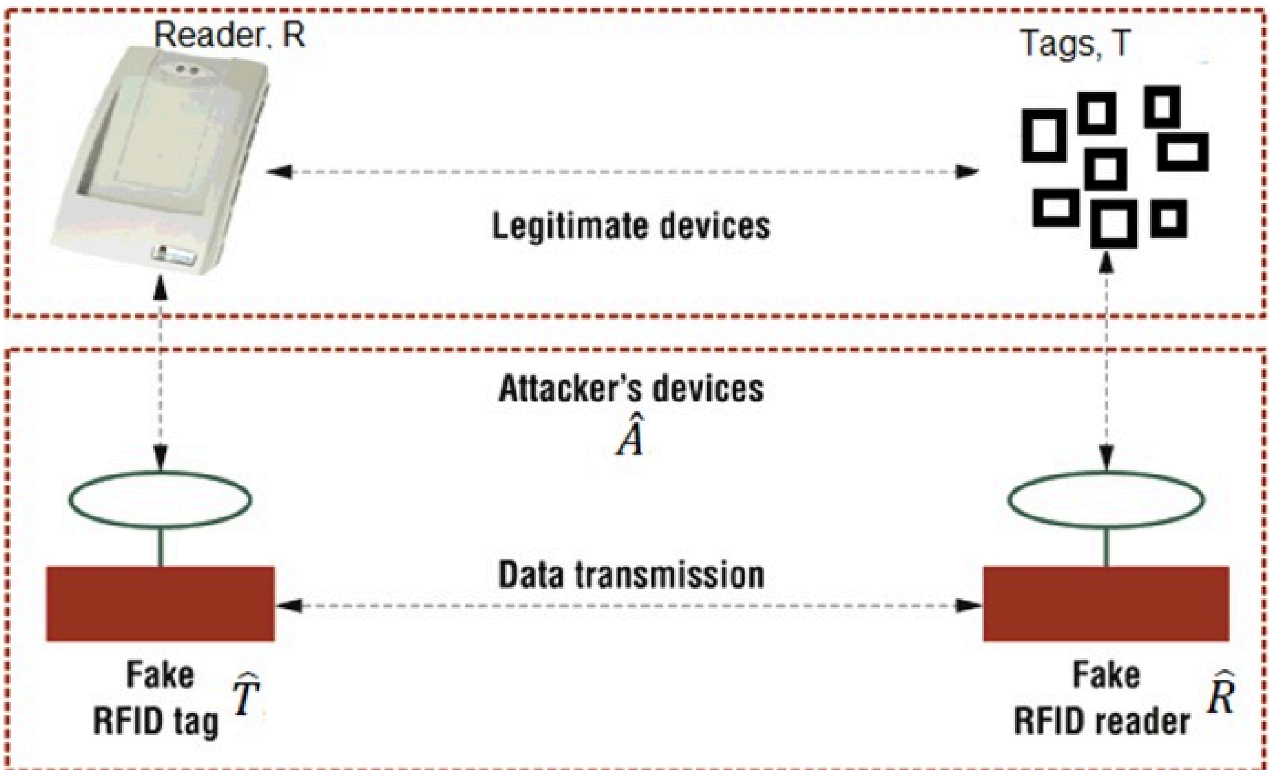


Fig. 4. Attack model in our system.

We assume that the adversary, the adversarial reader, and the adversarial tag have polynomially bounded resources. In addition, the adversary can launch physical attacks. However, the hardware-based defenses against physical attacks are beyond the scope of this paper. We also assume that the reader cannot be compromised.

6. Privacy model

In this section, we explain and theoretically define how AnonPri provides privacy and guarantees unlinkibility. At the end of the protocol description, we mention that this protocol provide unlinkability and thereby preserves privacy. The adversary cannot link the responses with the tags, even if she can decrypt the first portion of the response and learn the identifier that the tags are using to produce the response. Like Juels and Weis,[16] we use an experiment-based definition to formalize RFID privacy. We conclude that the adversary cannot break unlinkability or invade privacy with probability better than random guessing. In our system, the following oracle-like construction exists:

$\mathcal{O}_{pick}$ is an oracle that randomly chooses some tags from all the N tags of the system.

$\mathcal{O}_{encrypt}$ takes a tag T as an input. Given the nonce n_r, the group key k_G, the secret key k_T and the set of identifiers Ω, the oracle randomly selects an $ID \in \Omega$, generates another nonce and finally produces the response $\beta = (u, v)$. It outputs the cipher text β.

$\mathcal{O}_{query}$ is an oracle that, provided with a tag T, queries the tag and outputs the received response β.

$\mathcal{O}_{flip}$ is an oracle that, provided with two tags T_0, T_1, randomly chooses $b \in \{0, 1\}$ and queries the tag T_b using $\mathcal{O}_{query}$. Then it outputs the response β_b.

6.1. Information privacy against

Given a tag T, the set of identifiers Ω stored on T, and an identifier ID, an adversary can break the information privacy of our protocol if she can guess whether the tag T is using the ID. Moreover, ϑ is the security parameter and $t \in \mathbb{N}$ is the maximum number of time the adversary can query the tag T. In addition, since the oracles of our model are random, the inputs are computationally intractable from the outputs of the oracles.

Experiment $\mathrm{Exp}_{\hat{A}}^{priv}[\theta, t]$

1. **Setup:** The issuer initializes the N tags of the system with their corresponding unique secret keys, the group keys, and the sets of identifiers after dividing the tags into τ groups. It shares all the secret information with only the reader.
2. **Learning:** $\mathcal{O}_{pick}$ provides the adversary with a challenged tag T that the adversary queries t times and appends each response β to the list L (initially L is an empty list).
3. **Guess:** Now the adversary transmits the tag T to the oracle $\mathcal{O}_{encrypt}$ with a nonce and receives a response β from the oracle. The adversary selects an identifier ID. Given the list of t responses in L, $\hat{A}$ outputs 1 if she guesses that β is produced using ID, and 0 otherwise. $\hat{A}$ is successful if her guess is right.

Definition 1

AnonPri is said to preserve information privacy with security parameter ϑ and poly(ϑ) representing any polynomial function of ϑ, if $\forall \hat{A}, \Pr[\mathrm{Exp}_{\hat{A}}^{priv}[\theta, t]\text{succeeds}] \leq \frac{1}{2} + \frac{1}{poly(\theta)}$.

6.2. Unlinkability against

The adversary should not be able to distinguish between the two responses from the same tag.

Experiment $\mathrm{Exp}_{\hat{A}}^{unlink}[\theta, t]$

1. **Setup**: The issuer initializes the *N* tags of the system with their corresponding unique secret keys, the group keys, and the sets of identifiers after dividing the tags into τ groups. It shares all the secret information with only the reader.
2. **Learning:** $\mathcal{O}_{pick}$ provides the adversary with two challenged tags T_0, T_1 from the same group. The adversary queries each tag *t* times and appends each response β_0, β_1 to the list *L* (initially *L* is an empty list).
3. **Guess:** The adversary transmits T_0, T_1 to the oracle $\mathcal{O}_{flip}$. receives the response β_b from $\mathcal{O}_{flip}$. Given the list of responses *L* and the response β_b, the adversary guesses the value of b. $\hat{A}$ succeeds if her guess is right.

Definition 2

AnonPri is said to provide unlinkability with security parameter ϑ and poly(ϑ) representing any polynomial function of ϑ, if $\forall \hat{A}, \Pr[\mathrm{Exp}_{\hat{A}}^{unlink}[\theta, t]\text{succeeds}] \leq \frac{1}{2} + \frac{1}{poly(\theta)}$.

In our system, the adversary has no better way other than guessing to become successful in distinguishing the tags. Hence, the probability of getting successful in distinguishing the tags is less than or equal to 1/2. For example, let say, the adversary sends the oracle 2 inputs - m_0 and m_1. Oracle will choose one of them randomly and compute an output (Out_0) and send it back to the adversary. Note, here is the oracle works as a blackbox. Now, the adversary has no information other than m0, m1 and Out_0. If the adversary can now successfully find out Out_0 belongs to which input, she is able to break system's privacy. However, since the adversary has no other information, its best bet is to choose one of the input randomly with probability 1/2. If the input chosen is really the input corresponding to Out_0, then adversary breaks the privacy of the system, in other words the adversary is able to distinguish/link the tags with probability 1/2.

7. Security and privacy analysis

In this section, we formally prove that our protocol preserves data privacy and provides unlinkability. In addition, we analyze the preservation of privacy in some attack scenarios where some of the tags of the system are compromised by the adversary $\hat{A}$. We begin the section with the formal theorem on how AnonPri preserves privacy and provides unlinkibility. We also formally prove them in this section.

7.1. Information privacy

Theorem 1

AnonPri preserves information privacy with respect to the adversary $\widehat{A}$.

Proof

Let us assume $\mathcal{O}_{pick}$ provides the adversary $\hat{A}$ with a tag T. $\hat{A}$ transmits this tag to the oracle $\mathcal{O}_{encrypt}$ with a nonce n_1. Then $\mathcal{O}_{encrypt}$ provides $\hat{A}$ with the response β.

Now, $\hat{A}$ selects a *ID*. To break data privacy, $\hat{A}$ should tell if β is produced using the *ID*. This implies that $\hat{A}$ has to identify the input of the encryption by just learning the cipher text. $\hat{A}$ can succeed in two cases. First, if she can retrieve the inputs from the output of the random oracle. But this contradicts with our assumption that the inputs of a random oracle are computationally intractable from the output of the oracle. Second, if $\hat{A}$ knows the secret keys of the tag T. Without tampering the tag T, if $\hat{A}$ can determine the keys by learning the cipher texts, this again breaks the semantic security of the symmetric key cryptography. Therefore $\hat{A}$ can break data privacy with probability no better than random guessing. Thus, it proves data privacy property of Definition 1.

7.2. Unlinkability

Theorem 2

AnonPri provides unlinkability with respect to the adversary $\hat{A}$.

Proof

Let us assume $\mathcal{O}_{pick}$ provides the adversary $\hat{A}$ with two tags T_0, T_1 from the same group. These two tags go into the learning phase. $\hat{A}$ transmits T_0, T_1 to $\mathcal{O}_{flip}$ which outputs the response β_b.

Now, to break unlinkability, the adversary $\hat{A}$ has to tell the value of b. We assume that the adversary's guess is right. In other words, the adversary can determine whether the response β_b is produced by T_0 or T_1, given the learned responses from both the tags. The responses of a tag cannot be a signature of the tag because according to our protocol, a nonce on the tag side makes each response different from all the previous responses originated from the same tag. Therefore, we can say that the guess is right because the adversary knows the keys (the group key and the secret key) stored on these two tags. Without tampering the tags T_0, T_1, the adversary has to determine the keys stored on these tags by just observing the cipher texts. But this contradicts with the semantic security of symmetric key cryptography. Therefore, the adversary can break unlinkability with no better approach than random guessing. Thus, it proves the unlinkability property of Definition 2.

7.3. Physical attack

Under this attack (shown in Fig. 5), we consider that the adversary $\hat{A}$ can compromise any tag with a probability of $\frac{1}{N}$. Whenever a tag T_j becomes compromised, the adversary learns all private information stored on the tag T_j. Therefore, the adversary can now decrypt *u* of each response *β* originated from the other members of the group G_i. Thus, $\hat{A}$ can learn the identifier that a tag is using to produce its response by decrypting the *u*. We discuss the aftereffect of this attack with an example and demonstrate how AnonPri provides unlinkability even if the adversary realizes the identifiers used in the responses.

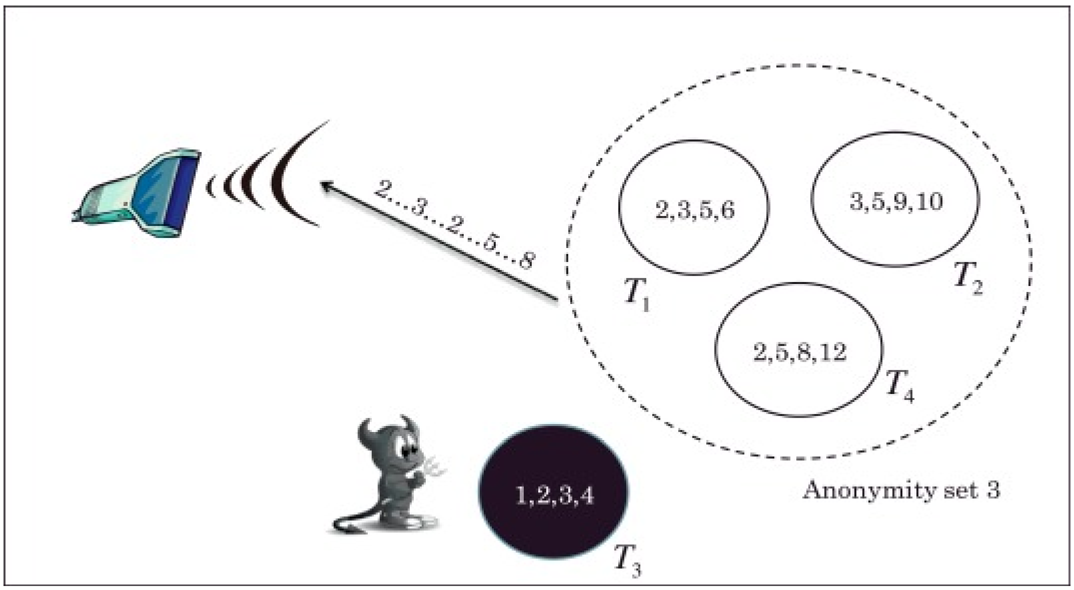


Fig. 5. After effect of a physical attack on AnonPri, where T_3 is compromised by the adversary.

We consider a group G_i of four tags T_1, T_2, T_3, and T_4. Suppose the adversary compromised the tag T_3 as shown in Fig. 4. Now the adversary learns the group key k_{G_i} , the tag secret key k_{T_3} and a set of identifiers $\Omega_3 = \{1,2,3,4\}$. From now on, the adversary can decrypt *u* part of all the responses originated from T_1, T_2, and T_4 with the group key k_{G_i}. But, the adversary still cannot decrypt *v* part of these responses since she does not possess the secret keys of these tags. With this learned information (k_{G_i} and Ω_3), the adversary tries to track the other tags of this group. Since the adversary can decrypt *u* of each responses, she can learn the identifier underlying the cipher text *u*. In other words, she can discover which identifier has been used to produce a response. The arrow in the Fig. 4 represents that the responses of the authentication sessions (after T_3 is compromised) are transmitted from the tags (T_1, T_2, T_4) to the reader. The identifiers used in these responses are shown on above the arrow. Each identifier is shown in plaintext since the adversary can retrieve the identifier by decrypting *u* of *β* using k_{G_i}.

According to our protocol, even if the adversary comes to know about the identifier used in a response, she cannot conclude which of the potential tags is the sender of this response. In our example, the adversary discovers the identifier 2 is used two times, but she cannot be certain which of these tags (T_1, T_2, T_4) is the originator(s) of these responses. Though T_3 shares the identifier 2 with only T_1 and T_4, however, the adversary has no knowledge about the parties with whom T_3 is sharing which of its identifiers. Even the adversary does not know how many of the identifiers of Ω_3 are being shared. So, under this scenario, the anonymity set of the potential senders of a given response seems to be 3 to the adversary. Therefore, when the adversary compromises one tag from the group of n uncorrupted tags, AnonPri forms an anonymity set of size 1 and another anonymity set of size $(n-1)$ from the group instead of n anonymity sets of size 1 like the group based authentication.[3] This noticeable partition improves the level of privacy provided by AnonPri. Because, the remaining $(N-n)$ tags of the system forms the other anonymity set which is same under both the protocols. Thus AnonPri prevents adversary benefit from tracking by compromising a tag.

We now consider the case of compromising multiple tags of the same group. In the above scenario, even if $\hat{A}$ compromises either T_1 or T_4 after compromising T_3, the adversary cannot be certain whether T_2 has identifier 2 in Ω_2 or not. Therefore, the size of anonymity set is still 2, i.e., , where c is the number of compromised tags of the group. If $\hat{A}$ compromises T_2 instead of T_1 or T_4, the size of anonymity set is still 2 (i.e., $n-c$). Therefore, we conclude that the anonymity set, formed from a group that is under physical attack, is of size $(n-c)$, where n is the group size and c is the number of compromised tags of the given group. AnonPri provides protocol-level privacy only. In real world, there are many possible side channels. If tags emit distinct "radio-fingerprint", then no protocol-level privacy countermeasures can prevent privacy infringement.[1]

8. Measurement of privacy

In this section, we measure the level of privacy achieved by AnonPri as a function of the total number of compromised tags. We consider two privacy metrics for the measurement of privacy. First, our privacy measurement technique is based on anonymity set like the privacy metric used by Avoine et al.[3] and we name this metric "privacy level". Second, we identify the amount of information disclosed by a scheme as another metric presented in.[25] This metric is based on Shannon's information theorem[33] and we name this metric "information leakage". From the perspective of AnonPri, these two are the most important metric since the main purpose of AnonPri is to provide privacy and ensure unlinkibility. Hence we choose these two metric for our experiment.

8.1. Measurement of privacy based on anonymity set

The level of privacy of an RFID system, achieved by a scheme, at a given time, is a function of the total number of compromised tags at that time. When some tags are compromised, the set of all tags are partitioned such that the adversary cannot distinguish the tags belong to the same partition, but she can distinguish the tags that belong to different partitions. Hence, these partitions become the anonymity sets of their members. The level of privacy based on anonymity set, $\wp$, can be measured as the average anonymity set size.[3]

$$\wp = \frac{1}{N}\sum_i |P_i|\frac{|P_i|}{N} = \frac{1}{N^2}\sum_i |P_i|^2$$

Where, $|P_i|$ denotes the size of partition P_i and $\frac{|P_i|}{|N|}$ is the probability that a randomly chosen tag belongs to partition P_i.

According to AnonPri, a similar kind of partitions is formed when tags become compromised. If c_i is the number of compromised tags within group G_i, then the set of the tags within this group is partitioned into c_i anonymity sets of size 1 and another anonymity set of size $(n - c_i)$. If $\mathbb{C} = \{c_i | c_i \text{is the total compromised tags with in } G_i\}$ is the set of compromised groups, $|\mathbb{C}|$ is the total number of compromised groups, and $C = \sum_{eachc_i \in \mathbb{C}} c_i$ is the total number of compromised tags, the level of privacy $\wp$ achieved by AnonPri can be expressed as

$$\wp = \frac{1}{N^2}((n(\tau - |\mathbb{C}|))^2 + \sum_{eachc_i \in \mathbb{C}} (c_i + (n - c_i)^2))$$

Where, N = total number of tags in the system

n = total number of tags within a group

τ = total number of groups in the system.

8.2. Measurement of privacy based on information leakage

We measure the information leakage in bits based on Shannon's information theorem.[33] If we have a group of tags of size S and the adversary divides this group into two disjoint subgroups of size $S/2$, then 1 bit of information is disclosed out of $\log_2 S$ bits. Extending this concept from two subgroups of equal size to two subgroups of different sizes, where $\frac{S}{a}$ tags are in one subgroup and the remaining tags $\left(1 - \frac{1}{a}\right) S$ are in another subgroup, we can measure the average amount of information disclosed in bits as follows

$$I = \frac{1}{a}\log_2(a) + \frac{a-1}{a}\log_2(\frac{a}{a-1}).$$

In general, if the adversary splits N tags of the system into k disjoint partitions, then

$$I = \sum_{i=1}^{k} \frac{|P_i|}{N} \cdot \log_2(\frac{N}{|P_i|})$$

Where, $|P_i|$ denotes the size of partition P_i.

According to our protocol, if $\mathbb{C} = \{c_i | c_i \text{is the total compromised tags within } G_i\}$ is the set of compromised groups, $|\mathbb{C}|$ is the total number of compromised groups, and $C = \sum_{each c_i \in \mathbb{C}} c_i$ is the total number of compromised tags, the amount of information leakage in bits I can be expressed as

$$I = (\frac{n(\tau - |\mathbb{C}|)}{N} \log_2(\frac{N}{n(\tau - |\mathbb{C}|)})) + \sum_{\text{each} c_i \in \mathbb{C}} (c_i(\frac{1}{N} \log_2 N) + \frac{(n - c_i)}{N} \log_2(\frac{N}{(n - c_i)}))$$

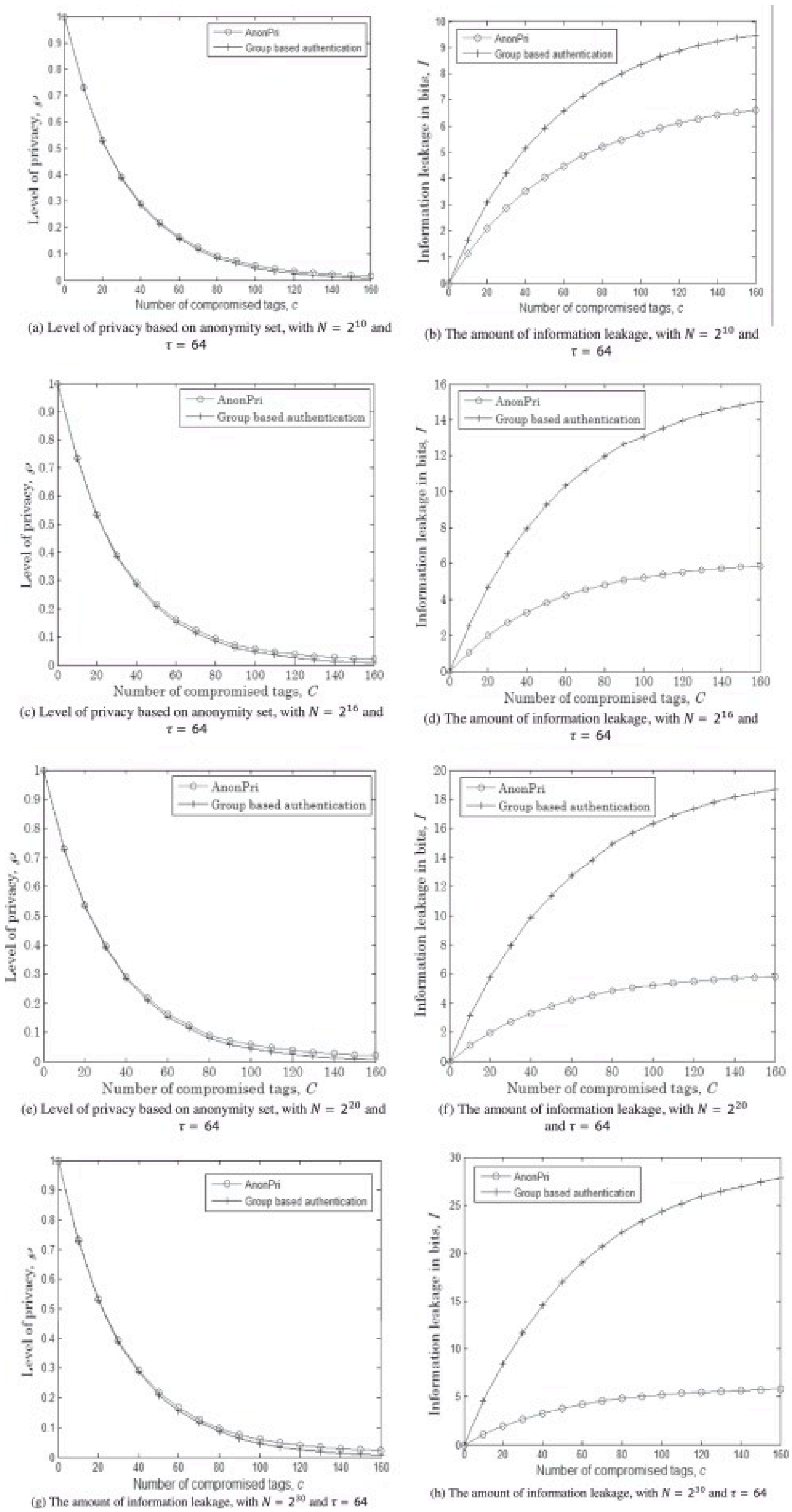
where, N = total number of tags in the system

n = total number of tags within a group

τ = total number of groups in the system.

8.3. Experimental results

We have compared both the protocols, AnonPri and the group based authentication, using a Matlab simulation. The experiment results establish that the level of privacy provided by AnonPri is higher than that of the group based authentication. Our comparison is based on the two metrics presented above, the level of privacy (based on anonymity set) and information leakage. We have come up with a conclusion similar as[25] that the information leakage describes the privacy threats better than the anonymity set. In our simulation, we have considered four systems with $N = 2^{10}, \tau = 64, N = 2^{16}, \tau = 64, N = 2^{20}, \tau = 64$ and $N = 2^{30}, \tau = 64$. Tags are selected to be compromised with a uniform random distribution. The number of compromised tags ranges from 0 to 160. We have run the simulation for 100 times and computed the average $\wp$ achieved by AnonPri and the group based authentication as a function of the total number of compromised tags C (see Fig. 6(a), (c), (e), and (g)). The small increase in the level of privacy achieved by AnonPri is visible when the number of compromised tags is more than 30.



(a) Level of privacy based on anonymity set, with $N = 2^{10}$ and $\tau = 64$

(b) The amount of information leakage, with $N = 2^{10}$ and $\tau = 64$

(c) Level of privacy based on anonymity set, with $N = 2^{16}$ and $\tau = 64$

(d) The amount of information leakage, with $N = 2^{16}$ and $\tau = 64$

(e) Level of privacy based on anonymity set, with $N = 2^{20}$ and $\tau = 64$

(f) The amount of information leakage, with $N = 2^{20}$ and $\tau = 64$

(g) The amount of information leakage, with $N = 2^{30}$ and $\tau = 64$

(h) The amount of information leakage, with $N = 2^{30}$ and $\tau = 64$

Fig. 6. Comparison of AnonPri with the group based authentication.

During the simulation, we have also computed the average amount of information leakage *I*, for both the protocols, as a function of the total number of compromised tags *C* (see Fig. 6(b), (d), (f), and (h)). The plots depict that AnonPri achieves a significant amount of improvement in privacy protection. With the increase in the total number of compromised tags *C*, the average amount of information disclosed by the group based authentication is quite higher than the information disclosed by AnonPri. In Fig. 6(d) ($N = 2^{16}$), when *C* becomes 160, the group based authentication discloses about 15 bits out of 16 bits of information, while AnonPri discloses about 6 bits of information.

The group based authentication discloses 56.25% more information than AnonPri in a similar setup. Fig. 6(f) ($N = 2^{20}$) shows that the group based authentication reveals almost 19 bits out of 20 bits of information and AnonPri reveals around 6 bits of information. This time the group based authentication discloses 65% more information than AnonPri. Based on the simulation results, we can conclude that the information disclosed by the group based authentication increases with the size of the system (as it is also seen in Fig. 6(h)); however, AnonPri shows consistency in the information leakage in both the cases.

Information leakage is a better metric to demonstrate the privacy threats in RFID systems than anonymity set. Though the improvement in $\wp$ provided by AnonPri against the group based authentication is not significant, however, we can say that AnonPri provides better privacy protection than the group based authentication, based on the results of the amount of information disclosed by these two protocols.

9. Discussion

In this section, we discuss the limitations of AnonPri.

9.1. Search complexity

According to AnonPri, the reader's complexity is slightly increased than the group based scheme.[8] After receiving the response $\beta = (u, v)$from a tag T_j, the reader searches for the correct group key to decrypt *u*. In the worst case, the reader has to perform this operation τ times. If such a group key exists, the reader can retrieve the identifier ID_{i,j_x} from *u*. Now, the reader has to search for the tag's secret key to identify T_j by decrypting *v* properly. The reader searches a key space of size $|\pi_x|$. Therefore, in the worst case, the reader's total complexity is $\tau + |\pi_x|$. In the best case, the size of π_x is 3 and in the worst case, it can be *n*, size of the group. But in the group based scheme, the reader's complexity in worst case is $\tau + 1$. Nevertheless, AnonPri is much better than the other schemes where the worst case reader's complexity is *N*, the number of total tags in the system. To provide improvement in privacy protection, we have to sacrifice this small increase in the complexity of the reader. Since readers are more powerful than tags, they can handle this increase in search complexity.

9.2. Memory complexity

According to AnonPri, tags need to store *m* number of identifiers along with the group key and the unique secret key. Though tags have limited resources, however, the increase in memory requirement is acceptable than the increase in computation and communication complexity. A smart RFID tags have memory capacity of 32 kBytes or more.[17] Even RFID tags with extended memory capacity are available at the market.[10] All these tags can store the information required for AnonPri.

10. Related work

Many private authentication techniques have been proposed to protect user privacy for RFID systems. Some of these schemes require the reader to test $O(N)$ keys to authenticate a tag, where N is the total number of tags in the system. Such a complexity is unmanageable in a large-scale environment. These techniques can be classified into two categories, non-tree-based approaches and tree-based approaches. Non-tree-based protocols usually perform linear search to find out a tag. The search complexity is $O(N)$, where N is the number of tags. Obviously, the linear search is not efficient in large-scale RFID systems that may have millions of tags.[30]

Another non-tree-based approach, Hash-lock[36] method uses the hash value of a key to identify a tag. A variation of Hash-lock needs exhaustive search through all IDs to identify a tag. However, hash-chain, researchers further reduced the search complexity to $O(N^{2/3})$.[9] This approach suffers from de-synchronization attacks. Dimitriou's protocol[9] defends against the de-synchronization attack though it is not secure against tracking attack. Henrici et al.[11] propose the triggered hash chains approach that alters the tag ID after each successful authentication. The main drawback of the non-tree-based approaches is the low search efficiency. To address the issue, tree-based protocols are proposed. Molnar and Wagner proposed an approach in[20] that reduces the complexity of authentication from $O(N)$ to $O(logN)$. This reduction is made possible by using a key-tree instead of a flat key space. However, this key-tree based private authentication scheme reduces the complexity of the authentication for the reader, there is a price to be paid for this gain in performance. The level of privacy provided by the scheme is quickly decreasing as more and more tags are compromised. Numbers of research have been conducted to find out a trade-off between the complexity and the level of privacy provided by the key-tree based scheme. This trade-off is identified and analyzed by Avoine et al. in.[2] by Buttyan, Holczer, and Vajda in,[4] and more recently by Nohl and Evans in.[25] These papers introduce privacy metrics and quantify the level of privacy provided by the key-tree based scheme when some tags are compromised. In addition, in,[4] the authors observe that key-trees that have different branching factors at different levels of the tree can provide a higher level of privacy, and they propose an algorithm to determine the optimal key-tree for a given number of tags and a given upper bound on the complexity of the authentication.

Avoine et al. proposed a group based private authentication scheme in[3] (later improved by Hoque el.al[14]) that improves the tradeoff between scalability and privacy by dividing the tags into a number of groups. One major limitation of this protocol is that the level of privacy provided by the scheme decreases as more and more tags are compromised. Lu et al. propose a RFID private authentication protocol (SPA).[18] which enables a dynamic key-updating for tree-based authentication approaches. Molnar et al. propose a new method[21] that supports delegation in the tag authentication. The tag owner can transfer the ownership to another party for authenticating valid tags. Similarly, the authors in[35] propose a server-free authentication protocol. It does not need backend server or database. However, this approach does not provide an efficient key searching mechanism for the backend application.

The authors in[24] discuss the unlinkability and the real world constraints in RFID systems. They define a link expression with real world constraints and propose a location-tracking model. The simulation results show the real world constraints have possibility that break the unlinkability. However, the authors did not consider the unlinkability issue from privacy violation perspective.

A lightweight RFID private authentication protocol, RWP, have been proposed in,[37] based on the random walk concept. The analysis results show that RWP effectively enhances the security protection for RFID private authentication, and increases the authentication efficiency from $O(logN)$ to $O(1)$. However, this technique is suitable for tags with high computational power as the technique requires tags to perform randomized hash functions.

Another authentication technique proposed by Zhou in[40] focuses on utilizing fewer resources on the tags for authentication. However, even though they we able to achieve more security and efficiency, their proposed approach did not focus on providing privacy for the users. HB-family protocols based on LPN assumption are also booming as one of the attractive candidates for secure low cost protocols based on EPC tags due to its security against quantum adversaries, efficient computational time and memory requirement etc. However, their focus was design a secure authentication protocol to meet the demand of low-cost tags.

In,[38] the authors proposed a protocol that enables the private identification of tags in the system with constant-time complexity based quadratic residue, and thereby addresses the problem of individual tag identification in large-scale RFID systems. However, the protocol is based on timestamp and hence unlinkibility cannot be ensured.

In the recent past, significant research has been conducted in developing RFID systems to ease the everyday life of human.[13,39,22,19, and 15] Even recently some research has been performed to devise accurate ways of determining indoor location.[32,23] But all of these researches mainly focused on developing the system itself, rather than focusing to consider the privacy impacts of installing those RFID systems in practical environment. In.[34] Sun et al. have presented methods to perform large scale authentication and combat attacks.

They proposed RSLA which provides both high authentication efficiency and a high privacy protection mechanism. RSLA relies on skip lists, a different data structure from the existing solutions. However, this protocol is not suitable to be deployed in low-cost tags. Sakai et. al. propose a novel distributed RFID architecture in.[31] In addition, they proposed a coding scheme, which when incorporated with the new architecture, works against a wide range of adversaries including the random guessing attack, correlation attack, ghost-and leech attack, and eavesdropping. However, this protocol even strongly secure, does not discuss much about how to preserve privacy or guarantee unlinkibility. Chen et. al. proposed an anonymous authentication protocol based on asymmetry principle for RFID systems.[7] The protocol reduces the communication overhead and online computation overhead for both the tags and the readers, which compares favorably with the prior art.

Table 1 summarizes the capabilities of the existing works discussed in this section, where N is the number of tags in the system.

Table 1. Comparison of existing techniques.

Reference	Complexity	Cloning resistance	Tracking resistance	Privacy protection
[26]	O(N)	Yes	Yes	Yes
[36]	O(1)	No	No	No
[20]	O(logN)	Yes	No	Yes
[3]	[1]O(γ)	Yes	Yes	Yes
[2]	$O(N^{2/3})$	Yes	No	Yes
[9]	O(logN)	Yes	No	Yes
[11]	O(1)	No	No	Yes
[21]	O(logN)	No	No	Yes
[35]	O(N)	Yes	Yes	Yes
Our Protocol	[2]$O(\tau + \lvert\pi_x\rvert)$	Yes	Yes	Yes

1. *γ* is the number of groups in the system.
2. In the best case, the size of π_x is 3 and in the worst case, it can be *n*, size of the group.

11. Conclusions

RFID systems can be useful for many applications if the system can guarantee consumer privacy as well as improve scalability. To address the tradeoff between privacy and scalability, we have proposed an anonymous private authentication protocol (AnonPri) in this paper. We have presented a brief comparison between the tree based hash protocol and the group based authentication protocol for RFID systems. A detail security and privacy analysis of AnonPri establishes that AnonPri preserves information privacy as well as unlinkability. In addition, AnonPri provides higher level of privacy than the group based scheme when the adversary compromises some of the tags. Even though the search complexity of AnonPri is little higher than the existing protocols, it is much better than performing linear search in the database to identify a single tag. Finally, we can say that AnonPri is suitable for many applications where privacy violation is a major point-of-failure. Our future work includes further reducing the costs of complexity, storage, increasing scalability. Another future work can be to determine an optimal tradeoff between the authentication complexity and storage required.

References

[1]G. Avoine, P. Oechslin **A scalable and provably secure hash based RFID protocol** Proceedings of the IEEE International Workshop on Pervasive Computing and Communication Security (PerSec 2005). USA (2005), pp. 110-114

[2]G. Avoine, E. Dysli, P. Oechslin **Reducing time complexity in RFID systems** B. Preneel, S. Tavares (Eds.), Selected Areas in Cryptography, LNCS 3897, Springer (2005), pp. 291-306

[3]G. Avoine, L. Buttyan, T. Holczer, I. Vajda **Group-based private authentication** Proceedings of the World of Wireless, Mobile and Multimedia Networks (WoWMoM 2007). Finland (2007), pp. 1-6

[4]L. Buttyan, T. Holczer, I. Vajda **Optimal key-trees for tree-based private authentication** Proceedings of the Privacy Enhancing Technologies Workshop (PET 2006), Springer (2006), pp. 332-350

[5]CASPIAN Press Release. Metro's decision to drop the loyalty card, 2004. Last accessed July 26, 2010 - http://www.spychips.com/metro/press-release-feb-27.html

[6]C. Chatmon, T. v. Le, M. Burmester **Secure anonymous RFID authentication protocols** http://www.cs.fsu.edu/~burmeste/TR-060112.pdf (2006)

[7]M. Chen, S. Chen **An efficient anonymous authentication protocol for RFID systems using dynamic tokens** Proceedings of the IEEE International Conference on Distributed Computing Systems (ICDCS). OH (2015), pp. 756-757

[8]C. Diaz, S. Seys, J. Claessens, B. Preneel **Towards measuring anonymity** Proceedings of the Privacy Enhancing Technologies Workshop (PET 2002). USA. (2002), pp. 54-68

[9]T. Dimitriou **A lightweight RFID protocol to protect against traceability and cloning attacks** Proceedings of the EAI International Conference on Security and Privacy in Communication Networks (SecureComm 05) (2005), pp. 59-66

[10]Fujitsu Report. Fujitsu develops world's first 64KByte high-capacity FRAM RFID tag for aviation applications, 2008. Last accessed June 2010. http://www.fujitsu.com/global/news/pr/archives/month/2008/20080109-01.html

[11]D. Henrici, P. Müller **Providing security and privacy in RFID systems using triggered hash chains** Proceedings of the IEEE Intentional Conference on Pervasive Computing and Communication (PerCom 08) (2008), pp. 50-59

[12]L. Hildner.**Defusing the threat of RFID: protecting consumer privacy through technology-specific legislation at the state level** Harvard Civil Rights-Civil Liberties Law Review, 41 (2006), pp. 133-176

[13]S. Hinske **Determining the position and orientation of multi-tagged objects using RFID technology** Proceedings of the Pervasive Computing and Communications Workshops (PerCom Workshops 2007). (2007), pp. 377-381

[14]M.E. Hoque, F. Rahman, S.I. Ahamed **AnonPri: an efficient anonymous private authentication protocol** Proceedings of the IEEE Intentional Conference on Pervasive Computing and Communication (PerCom 2011) (2011), pp. 102-110

[15]A. Ilic, F. Michahelles, E. Fleisch **Dual ownership: access management for shared item information in RFID-enabled supply chains** Proceedings of the Pervasive Computing and Communications Workshops (PerCom Workshops 2007) (2007), pp. 337-341

[16]A. Juels, S. Weis **Defining strong privacy for RFID** Proceedings of the Pervasive Computing and Communications Workshops (PerComW 2007), USA (2007), pp. 342-347

[17]A. Laurie **Practical attacks against RFID** Netw. Secur. , 2007 (9) (2007), pp. 4-7

[18] L. Lu, J. Han, L. Hu, Y. Liu, L.M. Ni **Dynamic key-updating: privacy-preserving authentication for RFID systems** Proceedings of the IEEE International Conference on Pervasive Computing and Communications (PerCom 07) (2007), pp. 13-22

1[9]M.S.I. Mamun, A. Miyaji **A privacy-preserving efficient RFID authentication protocol from SLPN assumption** Int. J. Comput. Sci. Eng. (IJCSE), Inderscience Publishers, 9 (2014), pp. 234-243

[20]D. Molnar, D. Wagner **Privacy and security in library RFID: Issues, practices, and architectures** Proceedings of the ACM Conference on Computer and Communications Security (CCS 04). USA (2004), pp. 210-219

[21]D. Molnar, A. Soppera, D. Wagner **A scalable, delegatable pseudonym protocol enabling owner-ship transfer of RFID Tags** Proceedings of the ACM SIGAPP Symposium On Applied Computing (SAC 05) (2005), pp. 276-290

[22]V.P. Munishwar, S. Singh, C. Mitchell, W. Xiaoshuang, K. Gopalan, N.B. Abu-Ghazaleh **RFID based localization for a miniaturized robotic platform for wireless protocols evaluation** Proceedings of the IEEE International Conference on Pervasive Computing and Communications (PerCom 2009) (2009), pp. 1-3

[23]L.M. Ni, L. Yunhao, C.L. Yiu, A.P. Patil **LANDMARC: indoor location sensing using active RFID** Proceedings of the IEEE International Conference on Pervasive Computing and Communications (PerCom 2003). (2003), pp. 407-415

[24]Y. Nohara, S. Inoue, H. Yasuura **Unlinkability and real world constraints in RFID systems** Proceedings of of Pervasive Computing and Communications Workshop (PerCom Workshops 2007) (2007), pp. 371-376

[25]K. Nohl, D. Evans **Quantifying information leakage in tree-based hash protocols** Proceedings of Information and Communications Security (ICICS 2006). USA. (2006), pp. 228-237

[26]M. Ohkubo, K. Suzuki, S. Kinoshita **Cryptographic approach to privacy friendly tags** Proceedings of RFID Privacy Workshop,, MA, USA, MIT (2003)

[27]Press Release: Invasion Of Privacy? RFID Tracking Kids On School Buses, URL: http://www.ibtimes.com/invasion-privacy-rfid-tracking-kids-school-buses-privacy-advocates-concerned-attendance-management [Last accessed: 3/28/2016]

[28]Press Release: RFID Tags - Smart Idea or Invasion of Privacy?, URL: http://www.streetdirectory.com/travel_guide/115640/technology/rfid_tags___smart_idea_or_invasion_of_privacy.html [Last accessed: 3/28/2016]

[29]F. Rahman, S.I. Ahamed, J.J. Yang, Q. Wang **I am not a goldfish in a bowl: a privacy preserving framework for RFID based healthcare systems** Proceedings of IEEE International Conf. e-Health Networking, Applications and Services (Healthcom 12). (2012), pp. 335-340

[30]G. Roussos, V. Kostakos **RFID in pervasive computing: ctate-of-the-art and outlook** Pervasive and Mobile Comp., Elsevier (2008)

[31]K. Sakai, M.T. Sun, W.S. Ku, T.H. Lai **A novel coding scheme for secure communications in distributed RFID systems** IEEE Trans. Comp. , 65 (February (2)) (2016), pp. 409-421

[32]A. Saxena, S. Ganguly, S. Bhatnagar, R. Izmailov **RFInD: an RFID-based system to manage virtual spaces** Proceedings of Pervasive Computing and Communications Workshops (PerCom Workshops 2007) (2007), pp. 382-387

[33]C. Shannon **A mathematical theory of communication** Bell Syst. Tech. J., 27 (1948), pp. 379-423 and 623-656

[34]M.T. Sun; K. Sakai; W.S. Ku; T. Lai; A. Vasilakos, ``Private and secure tag access for large-scale RFID systems'' In IEEE Transactions on. Dependable and Secure Computing., vol.PP, no.99, pp.1–1

[35]C. Tan, B. Sheng, Q. Li **Serverless search and authentication protocols for RFID** Proceedings of IEEE International Conference on Pervasive Computing and Communication (PerCom 07) (2007), pp. 3-12

[36]S. Weis, S. Sarma, R. Rivest, D. Engels **Security and privacy aspects of low-cost radio frequency identification systems** Proceedings of Security in Pervasive Computing (SPC 2003), 2802, Germany, Springer-Verlag (2003), pp. 454-469

[37]Q. Yao, Y. Qi, J. Han, J. Zhao, X. Li, Y. Liu **Randomizing RFID private authentication** Proceedings of the Pervasive Computing and Communications Workshop (PerCom Workshops 2009) (2009), pp. 1-10

[38]C. Yalin, J.S. Chou, H.M. Sun **A novel mutual authentication scheme based on quadratic residues for RFID systems** J. Comput. Netw., 52 (August 12) (2008), pp. 2373-2380 DOI=http://dx.doi.org/10.1016/j.comnet.2008.04.016

[39]G. Zecca, P. Couderc, M. Banatre, R. Beraldi **Swarm robot synchronization using RFID tags** Proceedings of Pervasive Computing and Communications (PerCom 2009) (2009), pp. 1-4

[40]J. Zhou **A quadratic residue-based lightweight RFID mutual authentication protocol with constant-time identification** JCM, 10 (2) (2015), pp. 117-123.